OIPE IAP22 NOV 29 2007 PATENT & TRADEMARK OFFICE

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): 915-008.021

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on November 20, 2007

Signature: /Lissette Ramos/

Typed or printed name: Lissette Ramos

Application Number	Filed
10/804,855	March 19, 2004

First Named Inventor: Lauri PAATERO

Art Unit	Examiner
2134	Andrew L. NALVEN

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant/inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [x] attorney or agent of record. Registration number 27,550.
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/Alfred A. Fressola/
Signature

Alfred A. Fressola
Typed or printed name

(203) 261-1234
Telephone number

November 20, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

- [x] *Total of One forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OIPE IAP22 NOV 29 2007 PATENT & TRADEMARK OFFICE

Attorney Docket No.: 915-008.021
Application Serial No.: 10/804,855

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Re Application of:

Lauri PAATERO	:	Confirmation No.: **7421**
Serial No.: **10/804,855**	:	Group Art Unit: **2134**
Filed: **March 19, 2004**	:	Examiner: **Andrew L. NALVEN**

For: ***Secure Mode Controlled Memory***

Mail Stop: **AF**
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Sir:

This Request for Review is filed in response to the final Office Action of August 21, 2007.

REMARKS

Claims 1-36 were examined by the Office and claims 1-36 were rejected. Applicant respectfully requests review of the final rejections to the claims in view of the following discussion. The Office has committed clear error by failing to establish that the cited references, Rindsberg and Herbert, et al, in combination suggest at least one of the limitations recited in the independent claims.

This Pre-Appeal Brief Request for Review is submitted along with a Notice of Appeal.

Overview of the Present Invention

The present invention relates to a method of enhancing program code security and more generally, data security, be it program code or otherwise, which data is to be executed or acted upon in an electronic device comprising a secure execution environment to which access is restricted. It is also directed to a corresponding system and computer program product.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service on **November 20, 2007**, below with sufficient postage as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Lissette Ramos

As noted in the Background section of the present application, various electronic devices require access to security related components. Within the secure execution environment is typically found a processor which is able to access security related components, including data which may be stored external to the secure execution environment (whether within the device or otherwise). Such devices are subject to malicious attack which may attempt to decrypt data stored external to the secure execution environment. Therefore, there is a need to insure that such data stored external to the secure execution environment be highly resistant to such malicious attack.

The basic idea of the present invention as disclosed and claimed is that at various times a new secret key is generated in the secure execution environment of the electronic device to which access is restricted. In addition, the method verifies in the secure execution environment, the integrity of data to be written into a storage wherein the data is to be executed in the electronic device, encrypting in the secure execution environment the data by means of the new secret key, and writing the encrypted data into storage. Thus, malicious attack of the encrypted data in storage is greatly minimized due to the encryption based on the repeating secret key and the verification of the data.

Claim Rejections Under 35 USC §103

At section 5 of the final Official Action, claims 1-5, 7, 9-11, 17-21, 23, 25-26 and 31-36[1] rejected under 35 USC §103(a) as unpatentable over US patent 6,970,565, Rindsberg, in view of US patent 7,149,901, Herbert, et al (hereinafter Herbert).

It is specifically asserted with respect to claim 1 that Rindsberg teaches the actions recited above except that it fails to specifically teach generating keys repeatedly. The Office asserts that Herbert teaches generating, in a secure execution environment of an electronic device to which access is restricted, a new secret key repeatedly and using the new secret key for encryption of files to be stored. The Office further asserts that at the time of the invention, it would be obvious to a person or ordinary skill in the art to utilize Herbert's key generation method with Rindsberg's secure downloading system because the combination offers the advantage of increasing the strength of the encryption by using multiple keys with smaller data samples. Applicant respectfully disagrees for the reasons presented below.

The Cited Art

Rindsberg is directed to a method for securely downloading and installing a program patch to a plurality of processing devices. The invention is particularly directed to situations where the program patch is transmitted over a communications channel that is particularly vulnerable to hacking (Rindsberg, column 6, lines 20-28). Initially, an encrypted program patch is transmitted to a device intended to receive the updated patch (Figure 3, step 91) where the patch program is decrypted using a shared key (Figure 3, step 94). In

[1] Section 5 does not identify claim 36 as being rejected, but in fact it is rejected as specifically enumerated in the detail rejection presented at section 6.

Rindsberg, the integrity of the patch is checked (Figure 3, step 96) to determine if it is from the intended source or if errors are present and if it is not from the intended source or if errors are detected, the patch is deleted from memory (Figure 3, step 104). If the integrity check on the patch passes (Figure 3, step 98), the clear text patch program is re-encrypted using a unique key 63 corresponding to a unique ID 62 burned into the device at the time of manufacturing, where the unique key is known only to the processor (Figure 3, step 100) (see generally, Rindsberg, column 7, lines 36-39 and column 8, lines 4-33).

Herbert is directed to a method for maintaining integrity and confidentiality of pages that are paged to an external storage unit from a physically secure environment (Herbert, Abstract and Figure 1). An outgoing page is selected to be exported from a physically secure environment to an insecure environment. An integrity check value is generated, such as by the integrity check engine 13 so as to generate an integrity check value for later comparison when the page of data is subsequently paged back in. The outgoing page is then encrypted using a cryptographically strong encryption algorithm via encryption engine 12 based upon a random number generator 18 used to generate keying material for the encryption engine. By use of the encryption and the integrity check, the security of the data on the outgoing page can be maintained in an insecure environment since when it is read back, it is integrity checked with the previously generated integrity check value. If the integrity check is good, the page is allowed to populate a secure random access memory 14 within the physically secure environment 1 (see generally Herbert, column 2, line 47 through column 3, line 16).

Discussion

As set forth in the final Official Action, the Office asserts that it would be obvious to a person of ordinary skill in the art at the time of the invention to utilize Herbert's key generation method with Rindsberg's secure downloading system. However, contrary to the position taken by the Office as discussed in the Response to Arguments section (section 4), it is respectfully submitted that a person of ordinary skill in the art at the time of the present invention who would like to increase the security of the downloading and installation of patch programs to several devices, would, if knowledgeable of the teaching of Herbert, not repeatedly generate a new unique key in the secure execution environment for purposes of encrypting data, but at best would use the encryption engine of Herbert to generate a new shared key that is used in Rindsberg for encrypting the patch program which is transmitted to all devices intended to receive the updated patch (see Rindsberg, column 8, lines 4-7). This statement is premised on the fact that in Rindsberg at column 8, line 67 through column 9, line 8 it states:

> "Since the shared key is typically known by a large number of devices, it is more likely to be compromised. Another reason that a second unique key is used is that the shared key may be changing at a relatively frequent rate. It is more efficient and practical to store the patch program encrypted using the permanent unique key rather than the transitory

shared key. This is especially true considering that a patch program may be in a service for relatively long periods of time".

This passage in Rindsberg makes clear that since the shared key is typically known by a large number of devices, it is more likely to be compromised and therefore it is more likely that a person of ordinary skill in the art would try to protect this relatively insecure key if one desires to increase overall security. Thus, if the idea of using a random number generator to encrypt a page of information as disclosed in Herbert is applied to the teaching of Rindsberg, it would be used for purposes of increasing the security of the shared key, since it is the shared key in Rindsberg that is used to encrypt the patch program that is distributed to multiple devices and therefore subject to the greatest chance for malicious attack. There would be no particular reason for using a random number generator for purposes of generating an encryption key for purposes of changing the unique key disclosed in Rindsberg. It is the unique key that is then used to encrypt the patch contents for purposes of storing in non-volatile memory associated with the device so that it can be later decrypted using the unique key of the device prior to loading the patch memory for execution by the processing device. At best, Herbert discloses encrypting an outgoing page by the encryption engine for storage in an insecure area so that when it is read back into the secure environment, it can be integrity checked and decrypted for use within the device.

Furthermore, it is specifically disclosed in Rindsberg that the unique key 63 used to re-encrypt the patch program is a key which is only known to the device itself and typically each such key corresponds to a particular unique ID 62 which is burned into the device during manufacture (Rindsberg, column 7, lines 36-39). If, as proposed by the Office this permanent unique key is changed, the device in Rindsberg may no longer be identified as having that particular unique ID. Furthermore, Rindsberg specifically claims the idea that the unique key is permanently burnt into the computing device (see, for example, claim 36) and thus there is no suggestion in the disclosure or claims of Rindsberg toward having a repeatingly altered unique key. This is in contradistinction to the argument presented at section 4 of the final Official Action where the Office asserts that a person of ordinary skill in the art would have combined Rindsberg and Herbert to modify the unique key of Rindsberg repeatedly.

The Office argues in the Advisory Action that a rotating key in Rindsberg would not change its operation since it could still be used to identify the device. But if this were so, then clearly Rindsberg would not teach burning the ID (and therefore the unique key) into the device at the time of manufacture.

In summary, the unique key in Rindsberg has the functionality of identifying the device. To repeatedly change that unique key would in effect negate this functionality (see Abstract of Rindsberg).

In fact MPEP §2143.01 VI addresses this situation.

"VI The Proposed Modification Cannot Change the Principle of Operation of a Reference

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facia* obvious. *In re Ratti,* 270 F.2d 810, 123 USPQ 349 (CCPA 1959)."

Here, as in the cited *In re Ratti* decision, to modify the unique key in Rindsberg which represents an identification of the device with a repeating new key would effectively negate the identification property of the unique key disclosed in Rindsberg.

In short, a person of ordinary skill in the art, would not under any normal circumstances be motivated to change the burned in unique key of Rindsberg repeatedly. Consequently, the particular combination asserted by the Office of using Herbert's key generation with the unique key disclosed in Rindsberg would not in fact be possible nor obvious to a person of ordinary skill in the art at the time of the present invention.

It is therefore respectfully submitted that Rindsberg fails to suggest the need or desire for repeatedly generating a new secret key that is used to encrypt in a secure execution environment data and writing that encrypted data into storage. The combination of Herbert with Rindsberg would not make up for this deficiency in Rindsberg since at best, Herbert teaches that a secret key can be generated by means of a random number generator, but does not suggest that such a secret key would be used for changing a unique key as disclosed in Rindsberg for encrypting data which has been previously decrypted by means of a shared key.

It is therefore respectfully submitted that claim 1 is not unpatentable under 35 USC §103 in view of Rindsberg further in view of Herbert.

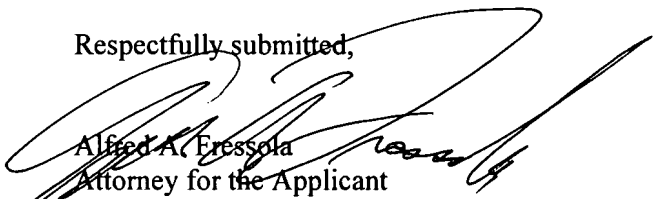
Independent system claim 17 and independent system claim 36 recite elements corresponding to those set forth in method claim 1 and therefore claims 17 and 36 are also not unpatentable under 35 USC §103 in view of Rindsberg further in view of Herbert.

All of the dependent claims are further distinguished over the cited art at least in view of their dependency from an allowable independent claim.

Conclusion

The rejections of the final Official Action having been shown to be inapplicable, withdrawal thereof is requested and passage to issue of the present application is earnestly solicited. The undersigned hereby authorizes the Commissioner to charge deposit account 23-0442 for any fee deficiency required to submit this response.

Respectfully submitted,



Alfred A. Fressola
Attorney for the Applicant
Registration No. 27,550

Date: November 20, 2007
Ware, Fressola, Van Der Sluys & Adolphson LLP
755 Main Street, P.O. Box 224
Monroe, CT 06468
(203) 261-1234
Customer No. 004955